DATA ENCRYPTION IN E-COUNSELLING SYSTEM (DEECS)

ATHIRAH FAYYADHAH OTHMAN

A report submitted in partial fulfillment of the
requirements for the award of the degree of
Bachelor of Computer Science (Software Engineering)

Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang

NOVEMBER 2009

DECLARATION

I declare that this thesis entitled "Data Encryption in E-Counselling System" is the result of my own research except as cited in references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree."

Signature : ……..
Name of Candidate : Athirah Fayyadhah binti Othman
Date : 24th November 2009

DEDICATION

To my beloved father and mother,
Mr. Othman bin Zainal Abidin and Mdm. Naziah binti Kamun,
who always give me a courage to finish this thesis.

To Mr. Abdullah bin Mat Safri thank you for the support, advices and helping hands to finish this project.

To Norlia Che Saad, Nurul Hidayah Abd. Rahim,
Che Wan Nurul Fatihah Che Wan Fadzal, Siti Munirah Abdul Kudus,
Muhammad Khalis Yalah
my friends and all faculty members
thank you for your supporting teaching.

ACKNOWLEDGEMENT

Firstly, thanks to Allah for the idea, good health to complete this project. In preparing this thesis, I was contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my thesis supervisor Encik Abdullah bin Mat Safri and my mother for his encouragement, guidance, critics and friendship. Without their continued support and interest, this thesis would not have been the same as presented here.

I'm very thankful to Universiti Malaysia Pahang (UMP) for providing good facilities in the campus. Librarians at UMP also deserve special thanks for their assistance in supplying the relevant literatures and guiding me in using e-library to find resources to develop project.

My fellow postgraduate students should also be recognized for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. This views and tips are useful indeed. To all my friends thank you for your support, valuable opinion and sharing ideas during the progress of this project. Finally, special thank and

continuous love to my family for their understanding, encouragement and support, towards the completion of my project.

ABSTRACT

Communication has changed dramatically in recent years and many people now use the internet as the central role in their contact with friends, family and work colleagues. This social side to the web has been very successful and already been used at modern country like America. It is almost the expected way to do business. Previously, all the information of student was recorded manually by counsellor on paper. So, it have no guarantee of the security that the information would not be stolen or read by someone else and no security mechanism to ensure such data be read or handled in secure manner. The purpose of this project is to apply symmetric key (secret key) for encrypted memo in order to secure counselling session. This technique overcomes the problem of security in counseling session to ensure such data be read or handled in secure manner. Therefore, confidentiality can be achieve in this project.

ABSTRAK

Komunikasi telah berubah secara dramatiknya dalam kebelakangan tahun dan kini ramai menggunakan internet sebagai peranan utama dalam berhubung dengan kawan, keluarga dan rakan-rakan sekerja. Aspek sosial ini kepada web telah berjaya dan digunakan di negara moden. Ia hampir ke arah jangkaan untuk membuat perniagaan. Sebelum ini, segala maklumat pelajar direkodkan dalam kertas secara manual oleh kaunselor. Jadi, ianya tiada jaminan keselamatan bahawa maklumat tersebut tidak akan dicuri atau dibaca oleh orang lain dan tiada mekanisme keselamatan untuk memastikan data tersebut dibaca dan diurusakn dalam aspek keselamatan yang betul. Tujuan projek ini adalah untuk aplikasikan kekunci simetri (kekunci rahsia) dalam memo untuk menjamin sesi kaunseling yang selamat. Teknik ini mengatasi masalah aspek keselamatan dalam sesi kaunseling untutk memastikan data tersebut dibaca dan diuruskan dengan betul. Oleh itu, keyakinan boleh dicapai dalam projek ini.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

ECS	E-Counselling System
DEECS	Data Encryption in E-Counselling System
AES	Advances Encryption Standard
DES	Data Encryption Standard
SDLC	Software Development Life Cycle
DFD	Data Flow Diagram
PHP	Personal Home Page
IDE	Integrated Development Environment
RDBMS	Relational Database Management System
ERD	Entity Relationship Diagram
JHEPA	Jabatan Hal Ehwal Pelajar
UMP	University Malaysia Pahang
SQL	Structured Query language
PSM	Projek Sarjana Muda
SHA	Secure Hash Algorithm
HMAC	Authentication Code
NIST	National Institute of Standard and Technology
IDEA	International Data Encryption Algorithm

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The project name is Data Encryption in E-Counseling System. It is about online counselling that counselor communicate with user through internet, to give emotional support, mental health advice or some other counselling service. The user of this project are counsellor and student. Data Encryption in E-Counselling System (DEECS) is viable alternative source when user do not have enough time to go to the counselling unit to make an appointment or not comfortable to share problem face to face with counsellor. Online counselling can also be an effective source of help if you are unable to schedule an appointment for any reasons such as be experiencing an illness or disability that makes it difficult to attend the service in person or have hearing problems or other difficulties and would prefer to use text based communication. User can meet a counsellor for personal counselling or advice, from the privacy of their own computer over the internet.

No need to make an appointment and go to counsellor office. Just dial up anytime, day or night, at home or at hostel, counsellor can respond when ready to and can take time in processing any changes that are taking place, before next counselling session. It could be one or more question, it could be by email, but for this project it is over encrypted memo, more safety and privacy.

Memo are encrypted by using secret key. All the data transmission between student and counsellor are encrypted. So no one else can access or know the content of discussion. In detail why security are important in this system because to ensure the confidentiality of information that will be accepted by authentic user and cannot be read by other user.

1.2 Problem Statement

Current system for counselling unit, all the information of student was recorded manually by counsellor on paper and save it into file. Paper might be disappear or torn. So, it have no guarantee of the security that the information would not be stolen or read by someone else. No security mechanism to ensure such data be read or handled in secure manner and there is no confidentiality of counselling information.

Counsellor need to find manually one by one to get back or revise the information of some student or previous case. It is not a big problem if it only involved small number of students but the number of student will increase year by year and the record of student also increase significantly. It will take time to find information needed by counsellor. Counselling unit need to make preparation to cater this problem.

No online system for counselling unit give counsellor a big problem to face many students at one time. In addition, the number of student are too many for the counsellor to cater the student problem. By using online system, student

can share their problem and counsellor can cater the problem as many as possible they can any time, any where and any number of student at the same time.

Usually, student have a pack schedule and they do not have enough time to go to the counselling unit only to make an appointment with counsellor. In addition, student need to make an appointment again and again if counsellor are not around by that time. Because of that, it will make student get bored and no more feel to meet counsellor to share the problem.

Not all student are brave to meet counsellor face to face to share their problem. Some student need time to find someone that they are trust to share their problem and usually this type of person willing to share their problem without meet counsellor in person. They are more comfortable to share problem without face to face.

Other than that, not all students are perfect. There are some student that handicap. Some of them maybe have a sound trouble or not able to walk by their own and need to use wheel chair. It is more difficult for them to meet counsellor in person directly. Followings are the key points of problem statement that have been stated and elaborated above :

i. Non confidential information
ii. Information stored are not systematic
iii. Student are too many for counselor to cater the problem
iv. Time constrain to make an appointment
v. Student not willing to meet counselor face to face
vi. Handicap student

1.3 Objective

The objectives of the research are to:

i. Apply secret key for encrypted memo in order to secure counselling session.

ii. Develop database system for counselling unit to record information of student and counsellor.

1.4 Scope

Scope of this project are :

i. Scope of Technique

- Symmetric Cryptographic Technique (secret key) will be use in this project to apply encrypted memo and secure system.

ii. Scope of User

- User of this project are counsellor and student.

iii. Scope of System

- This system is an online web based system

iv. Scope of Session

- Only for individual counselling session available for this proposed system

v. Scope of Data

- Data are memo (plain text to cipher text), session information, secret key (Advance Encryption Standard, AES).

1.5 Thesis Organization

This thesis consists of three chapters. Chapter 1 will discuss on introduction to system. Chapter 2 will discuss on literature review. Chapter 3 will discuss on methodology. Chapter 4 will be discussing about the implementations of the system. Chapter 5 will discussed about the data analysis, constraints and recommendations for further study. Finally, Chapter 6 will state the conclusion that briefly describes the system.

CHAPTER 2

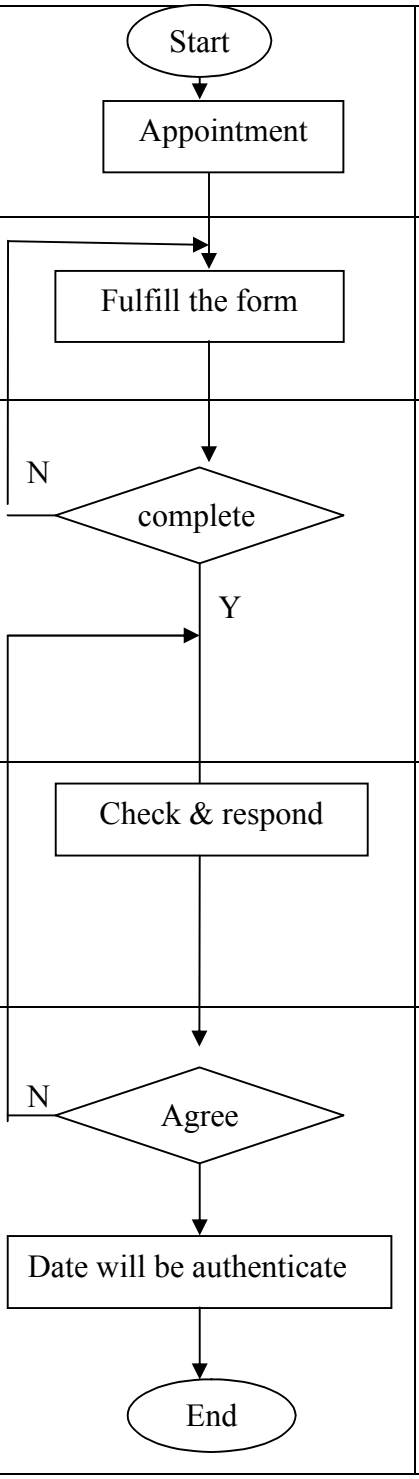
LITERATURE REVIEW

2.1 Introduction

In this chapter, it will show and discuss about the literature review, research about the system that has similar or related function with the E-Counselling. As an example, the system that similar to this project are online counseling, E-therapy and so on. In this chapter it will also describe about the technique and tools that are required and suitable to this project. All the information that required in this chapter can get from research on available similar project that have developed before this.

2.2 Current Implementation of Counselling System

Based on the study of the current system, there are weakness have been found about the manually system of counsellor unit. Normally in counselling session, long time are required to get information, to share and discuss a problem that student face it. During counselling session all the useful information are recorded manually by counsellor on paper. The paper might be disappear, torn or steal by someone. No security mechanism and there have no guarantee that the information are not steal or manipulate by someone. The information stored are not systematically. Counsellor need to find the information of certain student one by one if they want to revise the file again or to make the previous information as revision to new case. It will be a big problem and hard for counsellor if there have a large number of student record. After get all the useful information from the counselling session, counsellor make an analysis and come out with an early conclusion. Finally give the solution and motivation advised based on the problem occur. The flow process of the manual system for the evaluation method was shown in the Figure 2.10-2.12.



1. Student make an appointment at counsellor office.
2. Form will be accepted by counsellor assistant. Counsellor assistant will check the form first.
3. Information required are completed, form will be given to the counsellor for authenticate an appointment date.
4. If not, form will be given back to that student and they need to complete the form again.
5. A complete form will accepted by counsellor assistant. Counsellor assistant will check counsellor schedule and respond to that student.
6. If both student and counsellor agree with an appointment date, the date will be authenticate. If not counsellor assistant will give another suitable date that counsellor available.

Figure 2.10 : Flow process of apply an appointment